UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,924	04/26/2001	Craig S. Skinner	PALM-3609.US.P	8278

49637   7590   10/12/2005

BERRY & ASSOCIATES P.C.
9255 SUNSET BOULEVARD
SUITE 810
LOS ANGELES, CA 90069

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/844,924	SKINNER, CRAIG S.
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>01 August 2005</u> .

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-31</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-31</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>26 April 2001</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 4/28/2005 has been entered.

Response to Arguments

2.   In response to communications filed on 8/1/2005, applicant amends claims 1-5, 13, 14,

and 20-24. The following claims 1-31 are presented for examination.

2.1   The amendment to the abstract, filed on 4/28/2005 has been considered. However, the

abstract should not repeat information given in the title and should avoid using phrases which

can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention,"

"The disclosure describes," etc.. Therefore, the abstract is still objected.

2.2   Applicant's remarks, pages 11-13, filed on 4/28/2005, with respect to the rejection of

claims 1-31 have been fully considered, but they are not persuasive. Applicant indicates that

Beetcher's version field cannot be applied to the computer as a whole and therefore cannot

anticipate the claimed invention. However, the version field of Beetcher is only one of the

plurality of the entitlements disclosed. Beetcher also discloses other entitlements such as charge group, key type, serial number of the machine, and product entitlement field assigned to the device (see column 6, lines 20-40). In another embodiment, Beetcher discloses in column 7, lines 1-16, other authorization levels that are hardware specific. There is suggestion in column 2, lines 49-53 that other entitlement may also be machine specific entitlement or authorization level assigned to a machine to make sure that a software is authorized to run on a specific machine. Siefert also discloses key codes containing authorization levels (column 2, lines 40-65) and the key codes are assigned to an electronic device and authorizes said electronic device to run controlled applications according to the weighting levels described in column 4, line 44 through column 5, line 55. The cited art Beetcher either alone or in combination with Siefert teaches or suggests the claims as amended. Therefore, applicant has not overcome the rejection by amending the claims to recite that the first authorization level "is assigned to said electronic device". Upon further consideration, to render the claim rejection more obvious, claims 1-31 are now rejected in view of Beetcher and Siefert.

Specification

3.   The abstract of the disclosure is objected to because the amended abstract recites, "Specifically, a method and system for implementing a security technique that enables an electronic device to run controlled test applications is described", this language is not proper to the proper language of an abstract of the disclosure as explained below. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or

described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which

the invention was made.

4.1   **Claims 1-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent

5,933,497 to **Beetcher et al.** in view of US Patent 6,526,512 to **Siefert et al.**.

4.2   **As per claims 1 and 20, Beetcher et al.** discloses a method of security comprising the

steps of: enabling a computer system to execute a software module with an encrypted entitlement

key containing at least a machine serial number and version number that indicates sufficient

authority to execute that meets the recitation of a) enabling an electronic device to run a

controlled application with an encrypted record containing a copied serial number and a first

authorization level, for example (see column 6, lines 20-67); **Beetcher et al.** discloses that each

customer receives an entitlement key enabling the customer to run only those software modules

to which he is entitled (column 4, lines 40-45) that meets the recitation of wherein said first

authorization level authorized said electronic device to run controlled applications having

authorization levels not exceeding said first authorization level.   **Beetcher** also discloses other

entitlements such as charge group, key type, serial number of the machine, and product

entitlement field assigned to the device (see column 6, lines 20-40). In another embodiment,

Beetcher discloses in column 7, lines 1-16, other authorization levels that are hardware specific

assigned to said electronic device. There is suggestion in column 2, lines 49-53 that other

entitlement may also be machine specific entitlement or authorization level assigned to a

machine to make sure that a software is authorized to run on a specific machine. b) verifying

said electronic device is correctly enabled, for example (see column 6, line 65 through column 7,

line 47); and c) verifying said first authorization level is of sufficient authority to run said

controlled application on said electronic device, for example (see column 6, line 65 through

column 7, line 47); and wherein a second authorization level of said controlled application does

not exceed the first authorization level (column 7, lines 1-65). **Beetcher et al** suggests to add

protection by using entitlement that contains machine specific information and encoding it into

the software itself. **Siefert et al.** in an analogous art teaches key codes containing authorization

levels (column 2, lines 40-65) and the key codes (authorization levels) are assigned to an

electronic device and authorizes said electronic device to run controlled applications having

authorization levels not exceeding said first authorization level (see column 4, line 44 through

column 5, line 55). Therefore, it would have been obvious to one of ordinary skill in the art at

the time the invention was made to modify the method of **Beetcher et al** wherein the first

authorization level is assigned to the electronic device and authorizes the electronic device to run

controlled applications having authorization levels not exceeding the first authorization level as

taught by **Siefert et al** (see column 4, line 44 through column 5, line 55). One skilled in the art

would have recognized the advantage of preventing hacker from learning the identities of the key

codes and preventing hacker from learning how the security process run by assigning key codes

(authorization levels) to both the computer and the program by a match determination process

and using region of memory non-accessible to users to store the key codes (authorization levels)

as suggested by **Siefert et al** (column 7, lines 15-25 and column 7, line 55 through column 8,

line 35 and column 8, lines 59-67).

As per claims 2, 14, and 21, Beetcher et al. discloses the limitation of wherein step a)

comprises the steps of: a1) fetching a serial number uniquely associated with said electronic

device, said serial number located on said electronic device, for example (see column 7, line 47);

a2) copying said serial number, forming said copied serial number that is identical to said serial

number, for example (see column 6, lines 20-40); a3) creating a record that contains said copied

serial number and said first authorization level, said first authorization level previously assigned

to said electronic device, for example (see column 6, lines 20-40); a4) encrypting said record,

forming said encrypted record, for example (see column 4, lines 57-65 and column 8, lines 53-

65); and a5) storing said encrypted record in said electronic device, for example (see column 8,

lines 53-65). These claims are also rejected on the same rationale as the rejection of claim 1 for

reciting "said first authorization level previously assigned to said electronic device".

As per claims 3 and 22, Beetcher et al. discloses the limitation of wherein step b)

comprises the steps of: b1) locating said encrypted record, for example (see column 9, line 40

through column 10, line 20); b2) decrypting said encrypted record, if said encrypted record is

located, for example (see column 9, line 40 through column 10, line 20); b3) reading said copied

serial number from said encrypted record, if said encrypted record is successfully decrypted;

b4) fetching said serial number, for example (see column 9, line 40 through column 10, line 20);

and b5) comparing said serial number and said copied serial number, for example (see column 9,

line 40 through column 10, line 20 and column 13, lines 1-8).

As per claims 4 and 23, Beetcher et al. discloses the limitation of wherein step b)

comprises the further step of executing said controlled application on said electronic device, said

controlled application having controlled attributes, for example (see column 6, lines 40-67);

As per claims 5, 12, 24, and 31, the combination of **Beetcher et al** and **Siefert et al**

discloses the limitation of wherein said step c) comprises the steps of: c1) reading said first

authorization level from said encrypted record that is decrypted, if said serial number and said

copied serial number match, for example (see **Beetcher et al,** column 9, lines 40-67 and column

10, lines 20-67); c2) comparing said first authorization level with a second authorization level

assigned to said controlled application (**Beetcher et al,** column 10, lines 40-4 and column 7); and

c3) allowing access to said controlled attributes of said controlled application, if said first

authorization level is of an equal or higher authorization level than said second authorization

level, for example (see **Beetcher et al**, column 10, lines 20-47 and column 4, lines 34-46).

Siefert et al also discloses comparing first authorization level with second authorization level to

authorize the computer to run controlled applications as discussed in claim 1. Therefore, these

claims are also rejected on the same rationale as the rejection of claim 1.

    As per claims 6, 15, and 25, Beetcher et al. discloses the limitation of wherein step a) is

performed with object code instructions that meet the recitation of an enabler application, said

enabler application enabling said electronic device to run applications having authorization

levels equal to or lower than said first authorization level, for example (see column 8, lines 48-67

and column 4, lines 34-46).

    As per claims 8, 9, 18, 19, 27, and 28, the combination of **Beetcher et al** and **Siefert et**

al discloses the limitation of comprising the further step of: aborting said application and

denying access if any of the following conditions are met: said encrypted record is not

successfully located in step b1) ; said encrypted record is not successfully decrypted in step b2);

said serial number and said copied serial number do not match in step b5); or said first

authorization level is of a lesser value than said second authorization level in step c2) , for

example (see **Beetcher et al**, column 8, lines 48-67 and column 4, lines 34-46 and column 10,

lines 20-67).

Claims 13 and 16 contain some of the limitations of the rejected **claims 1-5**. Therefore,

claims 13 and 16 are rejected on the same rationale as the rejection of **claims 1-5**.

As per claim 17, Beetcher et al. discloses the limitation of wherein the same

encryption/decryption protocol is used in performing steps c) and m), for example (see column

13, lines 5-18).

As per claims 7 and 26, Beetcher et al. substantially teaches the claimed method of

claims 6 and 25. **Beetcher et al.** does not explicitly teach removing said enabler application

from said electronic device after successfully completing step a). However, **Siefert et al.** in an

analogous art teaches control access to enhance security of resources where a match

determination process can take actions of erasing part or all of the program to defeat running of

the program, for example (see column 7, lines 35-40). **Siefert et al.** also adds, hiding

process/codes or removing or placing them in separate memory or non-accessible memory

locations can prevent hackers to trace the logic of codes, for example (see column 7, line 40

through column 8, line 5). Therefore, it would have been obvious to one of ordinary skill in the

art at the time the invention was made to modify the method of **Beetcher et al.** to remove said

enabler application from said electronic device after successfully completing step a) as taught by

Siefert et al. One skilled in the art would have been lead to make such a modification because it

would make the security process non accessible to hackers, as suggested by **Siefert et al** for

example (see column 7, line 40 through column 8, line 35).

As per claims 10-11 and 29-30, Beetcher et al. discloses locking in memory the version

number the product number, serial number etc. and also discloses codes stored in read-only

memory (ROM) to make it not capable of alteration by customers, for example (see column 7,

lines 15-30 and column 9, lines 49-67). It is well known in the art of computer security that

computers have flash memory and using a flash memory will not depart from the spirit and scope

of the invention of **Beetcher et al.. Siefert et al.** also discloses using read-only memory (ROM)

for the encrypted data and serial number. Therefore, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to store said encrypted record and

serial number in locked flash record in said electronic device as suggested by **Beetcher et al.**

One skilled in the art would have been lead to make such a modification to prevent alteration of

these data by customers.

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The

examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin

Patent Examiner

October 5, 2005